

OS REGISTRY

8-0732X

19 May 1988

MEMORANDUM FOR: Deputy Director for Intelligence  
Director of Security  
Director of National Collection

VIA: Director of Scientific and Weapons Research *60*

FROM:   
Chief  
Technology Transfer Assessment Center

STAT

SUBJECT: Industrial Security as Viewed by the Aerospace Industry  
Association

25X1

1. On 9 May I attended the Industrial Security meeting of the Aerospace Industry Association in Tucson. I had been invited by Jed Selter, Director of Security for Boeing (Commercial)--the incoming Chairman of the Industrial Security Subcommittee--to speak on recent developments in the technology transfer problem. A copy of my "off the record but unclassified" remarks is attached.

25X1

2. Most interesting about the session was the debate over the attached draft National Industrial Security Program by the AIA.

-- They engaged in some self-flagellation, noting that as an association they should have done this five to seven years ago but because money was flowing in and their budgets were expanding, they took the easy way.

-- Now, the budget crunch is starting to hit. They argue that the goal is better security for less tax money; the principal concern, however, is clearly overhead problems for the corporation.

25X1

3. Our exposure to the industrial security problem from our corporate awareness program suggests many of the AIA complaints are justified.

-- They do get conflicting guidelines from the Services, DIS, NSA, and CIA.

-- Many of the rules are designed to address unsubstantiated threats (broad tempest rules, for example).

25X1

25X1

-- Most of the focus is on physical security, not on a broader security program. [redacted]

25X1

SUBJECT: Industrial Security as Viewed by the Aerospace Industry Association [redacted]

25X1

4. A major complaint is that US sponsored training programs on security and on the Soviet threat are badly done. They complimented CIA, noting we had the only believable threat briefing because it focused on what the Soviets really want, on whom they target, and on what techniques they use. AIA said DIS has the worst; the CEO at Grumman ordered his Director of Security never to schedule another DIS briefing at Grumman, according to the Director of Security. The FBI also got low marks. I noted that we were working with the DIS training staff in Richmond to help improve their briefings. [redacted]

25X1

5. On balance, the AIA plan has merit. An accepted, understandable system that reduced the administrative burden on the government, cut costs to industry, and focused on the true Soviet threat would benefit everybody but Moscow. I briefed TTIC on this initiative and at the request of several TTIC members will set up a meeting between AIA and TTIC so that TTIC can hear the Association's views. Other participants would be welcome. [redacted]

STAT

Attachments

Industrial Security meeting remarks  
Speech draft

25X1

AIA: TOWARD AN INTEGRATED NATIONAL  
INDUSTRIAL SECURITY PROGRAM

The United States Government/Industry team has a serious problem with the current industrial security program. The heart of the problem is the lack of coherent, strategic approach.

The procedures for protecting information, equipment, facilities and personnel, driven independently by different government user organizations, raise issues of uniformity and effectiveness. Comparatively, requirements among similar classified activities are fragmented and uncoordinated, unclear, inconsistent and often redundant. This is not cost effective. The program presently allows for differences among government agencies in inspection criteria with significant variances among district, field, and regional elements. At its worst, the program allows for the personal whim of government representatives in directing contractor activity voiced as official government requirements interpretation.

The situation is aggravated in that security standards applied to government entities are significantly lower than those applied to industry. This promotes a "do as I say, not as I do" environment, diluting the validity of established requirements and consistency required for professional results. The existence of redundant programs that have unclear direction and that lack timely and clear definition of the threat against which security measures should be established causes lack of confidence in the system by both government and industry. Security must be recognized as having a total systems impact on quality, cost and cycle time. An appropriate, practical approach to ensure efficiency, effective cost management, and guarantee accountability does not exist. The program, rather, encourages fire drill responses. There is no consistent baseline against which to professionally establish a cost effective safeguarding level, nor a performance means against which to measure compliance to minimum requirements.

With the present high visibility concerns in government and industry on cost and return on investment, resulting from both national and international economic pressures, the time is appropriate to establish a National Industrial Security Program. Evidence of breakdowns in the national security system uncovered in recent successful foreign intelligence activities further emphasizes this need.

A National Industrial Security Program should, at minimum:

- Be given a national priority.
- Be implemented by LAW rather than by Executive Order.
- Be developed by a Government/Industry joint Commission.
- Be placed at a level to encompass all agencies of the Government in their economic interface with industry - domestic and foreign.
- Be based on identifiable threats that include theft of intelligence, engineering and manufacturing techniques, product and process design.
- Not only be directed at protecting defense information, but include the protection of commercial development techniques that protect the economic interests of the Nation. *(key point)*
- Be reviewed constantly to ensure that its elements enable rather than disable industrial advances that strengthen the Nation's economic as well as military stature.
- Provide for and promote complete automation of good practices and good methodology to boost productivity.
- Have as its base a superior training standard for all participants. *(arrow points to "participants")*
- Not depend upon societies or private organizations outside of a central control system, and
- Reward cost effective but superior protection systemology.

// This National Industry Security Program, in summary, needs to provide for better national defense for fewer tax dollars through the demonstrated commitment to professionalism and excellence. //

Technology Transfer and National  
Security: An Update and Status Report



STAT

Chief

Technology Transfer Assessment Center

For: Aerospace Industries Association

May 9-11 1988

Tucson, Arizona

Good Morning. I am pleased to be here. If you have been following the press reporting on the Trade Bill that the President has said he will veto and the Toshiba sanctions that are in the Bill, you probably can tell that I am pleased to be almost anywhere than Washington. Depending on which press account you read, I am

- The principal Jap-basher in Washington
- The primary meddler complicating export control policy
- Somebody trying to usurp the functions of Commerce and State.
- The leader of an anti-Japanese cabal at CIA
- The last defense against godless communism.

Several of my superiors suggested I am all of the above. All of this press play--despite the fact that CIA does not crave publicity--reflects the political fallout from our

discovery of the first Toshiba/Kongsberg case and more recently our evidence that the parent firm Toshiba Corporation has, despite claims to the contrary, also transferred technology to the Bloc.

Nonetheless, in reality what all this debate shows is that the issue of technology transfer continues to be a major problem. Indeed, this is not new. Since the early days of the Reagan Administration few issues have had a higher policy priority, more visibility, or prompted as much debate and disharmony between key sectors in the US and between the US and its Allies than technology transfer to the Warsaw Pact. Depending on your point of view, the CIA has either hurt or helped the debate on technology transfer. For example, a few people have actually said the US would be better off if we had not uncovered the Toshiba/Kongsberg case. In any event, we have played a major role in the technology transfer issue.

Our biggest role has been as collector and analyst. Twice in the past few years we have made a large volume of facts openly available about the Soviet effort to acquire technology and provided analytical conclusions about the impact of this effort on the East-West strategic balance. The data and analysis have revealed a number of important points.

First, it is clear that the proscribed countries-- principally the Soviet Union and others in the Warsaw Pact, but also China, North Korea, and Libya--have large scale programs to acquire--both legally and illegally--Western equipment and technology to enhance their military. The evidence is overwhelming; much of it is discussed in detail in the publication Soviet Acquisition of Militarily Significant Western Technology: An Update. Although, released by Secretary of Defense Weinberger in September 1985, it is one of the worst kept secrets in Washington that CIA wrote it.

Second, from the scope and volume of transactions we have observed, it is clear that the Soviet appetite for Western technology is enormous.

-- In the late 1970s and early 1980s, the Soviets collected 6,000-10,000 hardware items and 100,000 documents annually to improve designs of future weapons systems and help develop countermeasures for Western systems. Most of this technology was of US-origin and you have been the principal target.

-- To bolster the actual production of weapons systems, the Soviets acquired illegally hundreds and in some cases thousands of machine

tools, computers, and microelectronic manufacturing equipment.

- To enhance their own equipment and in some cases weapons systems, they acquire at least 50 million ICs illicitly each year.

Third, the benefits, for at least the Warsaw Pact, have been tremendous.

- In the early 1980s, for example, more than 5,000 military related projects annually in the Soviet Union benefited from Western hardware and technical documents.
- In terms of specific weapon systems, we have seen the impact of purloined Western technology in Soviet radars, guidance systems, cruise missiles, anti-submarine weapons, laser-guided artillery shells, and anti-tank missiles to name a few.

Fourth, our analysis shows that the tactics used to acquire this equipment and technology fall into three fairly clear channels and require three very different policy responses.

- The open source channel is by far the largest channel, in terms of volume. We judge Moscow acquires at least several hundred thousand documents a year legally, through open source. This is by far the most difficult channel for a democracy to deal with; it may be that controls would cost us more than the Soviets.
- The illegal trade channel, which does not affect most of you in this room, is easy to identify but hard to stop. Here, the Soviets hire Western businessmen to violate export control laws and acquire large volumes of dual use hardware to produce military related items and in some cases weapons. The difficulty is in selecting what to control and in convincing our allies to enforce controls.
- The intelligence channel is the easiest to identify a solution for but hard to implement. For you it is the most important, because the aerospace industry remains Moscow's principal target. In this channel Soviets recruit assess

agents in the classic intelligence mode, looking for technology in its purest form--blueprints, company proprietary material, tech documents, and classified reports.

Some of our analysis of how, why and what the Soviets acquire has made people mad, sometimes at me. Indeed, the technology transfer issue may be the classic example of the problems facing CIA in providing intelligence support to policymakers. As Deputy Director of CIA Robert Gates pointed out in a recent article in Foreign Affairs, when our information and analysis supports the preconceived views of policymakers they praise it; when it does not they often accuse us of doctoring the information or of being biased in our judgments.

-- Our discovery and analysis of the Toshiba/Kongsberg case helped US policymakers push Japan and Norway into improving their export control laws but also has acquired for me the label of "Jap-basher" by some in Tokyo and Washington.

-- Our research showing that key COCOM countries lack the means and in some cases the will to enforce export controls did not make us many friends overseas. In the early 1980's,

West Germany was particularly displeased to be labelled by us--through a leak in Jack Anderson's column--as the number one source of trade diversion to the Soviet Bloc. By the way, despite their displeasure West Germany remains the number one diversion point today.

-- Our data shows that the Soviets still want US technology and equipment more than any other source. Although this is a vote of confidence in US technology, it also undercuts industry efforts for wide spread decontrol of their products.

I should say, by the way, that the response in the aerospace industry to our analysis showing you as the number one targeted industry has been uniformly positive. You have acknowledged the problem and taken steps against it. I will give you some more good news in a few minutes. The only criticism I have heard is from individual companies that complain that they were lower on the Soviet targeting list which we published than their competitors. After merging with another company on form actually called and asked if that boosted them higher on the list.

## A Status Report

Now that I have brought you up to date on our analysis of the Soviet acquisition effort, I would like to give you our assessment of how well the free world has done against this effort. In 1985 we wrote that "much can be done to stem losses because much is known about Soviet efforts; it is not an insurmountable problem." How much progress have we made. In one regard--education--we have been remarkably successful. We began in the early 1980's to try to convince people that the Soviets were actually stealing us blind. We now believe that virtually everyone who is convincible is convinced. The debate is now over what to do and whether we and our Allies have the political will to do it and are willing to pay the economic costs.

Against the illegal trade channel, the record is mixed. Our evidence shows that the Soviets have little trouble getting individual items--computers, microelectronics equipment, machine tools--but the volume is well below what they need in most cases. In many critical areas, however, the multilateral system of export controls has broken down. Too many, for example, of our successes are arrests of people after the equipment is shipped and the harm is done. The reasons for these failures are complex and would take much of my time and yours so I will leave this issue to the

question and answer period if you are interested. The details of the Toshiba case, itself, are fascinating and someday will make a great book.

In the area closest to your interests--espionage and industrial security--I have more good news for you and some bad news.

The good news is that we have evidence that suggests we have raised the cost and made it more difficult for Moscow to collect militarily critical technology through this channel. We, for example, have been able to disrupt collection and targeting by Soviet intelligence officers. Since the early 1980s, more than 400 Soviet intelligence officers have been expelled from posts around the world, the most recent in Sweden last week. The number would be even higher if East European intelligence officers were included. Many of these expulsions were for espionage related to technology transfer.

From your point of view, I have even better news. We judge that industrial security has improved significantly in the US in recent years and this, perhaps more than expulsions, has raised the cost to the Soviets. Many of you in this room deserve credit. For example, the visibility

and awareness of the problem is higher now in the defense industry. That, as you know, is critical because you are the primary target of this Soviet-program.

Now that I have given you a warm, glowing feeling, I will tell you the bad news. We believe Soviet efforts to collect technology must increase and your job and my job is going to get harder. The Soviets really have little choice.

- Even with their current collection effort, the gap between Warsaw Pact and Western foundation technologies such as microelectronics and computers is already growing.
- The US defense buildup of the 1980's has put more pressure on the Soviet military.
- Specific programs such as SDI have added to the Soviet problem. Not only do they need to collect to support their own strategic defense philosophy, the US program now forces them to collect to understand what we are doing.

Many scholars argue that Gorbachev's reforms are designed to spur the Soviet economy and its domestic R&D capabilities. That is true. The problem--from the Soviet view--is that first the reforms have to work--and that remains an open question--and second, the military cannot wait long. If Moscow went completely "cold turkey" off Western technology in the military area, the gap between the US and the USSR would accelerate.

I do not want to paint too gloom and doom a picture for Moscow. They have strengths in this technology race. First, their collection effort is by any measure a winning game for them and we believe they will continue. The recent Toshiba/Kongsberg case is a classic example of Soviet success. Through espionage they identified a problem they had with submarine noise; apparently through espionage they acquired designs or ideas for a new propellor; through export control violations they obtained the means to produce these propellers in large numbers. As a result, the Soviets are now where we thought they would be in the mid-1990's in terms of submarine quietness.

The Soviet's second strength is that they are more aggressive in applying technology to weapons systems than we are. As a result, their best technology gets into systems earlier; because of this the Soviets can tolerate a lag in the civilian sector and still match us weapon to weapon.

For example, we developed a 64K-RAM years before the Soviets but they will field weapons with this technology included about the same time as we do.

We have come a long way since the 1970's when COCOM was a vacation post for State, when the Intelligence Community largely assumed that the Soviet system was too inefficient to use what they stole, and US industry cared little about protecting key technologies. We cannot, however, rest. The Soviets cannot and will not.

On this the intelligence evidence is clear. The Soviets were stealing your technology during the last period of detente; they will be trying to steal it again.

Thank you. I would be glad to answer any questions you have.

OS REGISTRY

17 MAY 1988

## ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Information Technology Equipment Census

FROM

Chief, DDA Management Staff  
7D18 HQS

EXTENSION

NO.

DDA 88-1073

DATE

16 May 1988

STAT

STAT

TO: (Officer designation, room number, and building)

DATE

OFFICER'S  
INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1.

Director, Security

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

FYI -- OIT will also be surveying  
all DA Offices.

STAT

STAT

FORM  
1-79

610

USE PREVIOUS  
EDITIONS

★ U.S. Government Printing Office: 1985-494-834/49156

SECRET

~~ADMINISTRATIVE - INTERNAL USE ONLY~~

OIT-0356-88

2 May 1988

DDA/REG  
LOGGED

OS REGISTRY

17 MAY 1988

MEMORANDUM FOR: Executive Director  
Deputy Director for Intelligence  
Deputy Director for Operations  
Deputy Director for Science and Technology

VIA: Deputy Director for Administration

FROM: Edward J. Maloney  
Director of Information Technology

SUBJECT: Information Technology Equipment Census

1. The Office of Information Technology (OIT) requests Directorate participation in a census of the Agency's Information Technology (IT) equipment. The resulting inventory will be extremely useful for planning and analysis purposes for both OIT and the Directorates. It will identify equipment shortfalls and allow planning for future workloads and compatibility. OIT will also use the data to validate our equipment and maintenance database which is used to support and provide property accountability for much of the equipment in your components. In addition, we will be surveying customer modems in order to develop a better understanding of certain engineering and security issues. Component inventories will of course be made available to your staffs for their own planning and analysis.

2. For the purpose of this census we have grouped the Agency's IT equipment into three classes: office systems, word processing devices, and multiuser computer systems. Office systems are defined as terminals, personal computers, printers and plotters. Word processing (WP) devices have been identified as any WP-related terminals, printers, and special purpose computers. (Since the Wang equipment inventory is considered accurate, Wang devices are excluded from this census.) Multiuser computer systems have been separated into two categories. Departmental computers are defined as being capable of supporting two-to-twenty concurrent users. Large computers have been identified as those capable of supporting greater than twenty concurrent users. Simultaneously, we are also surveying customer modems. Modems are generally used for unclassified data communications with outside databases. The Office of Security is interested in both the

STAT

~~ADMINISTRATIVE - INTERNAL USE ONLY~~

~~ADMINISTRATIVE - INTERNAL USE ONLY~~

number, types and uses of these potentially vulnerable devices. There also may be some technical means of using the PBX to provide more efficient modem services. We need hard data, however, before we can engineer a solution.

3. To minimize the impact to your staffs, we are using existing OIT data as a starting point. These data have been extracted from OIT's PBX survey database, which encompasses all Headquarters equipment surveyed preparatory to being connected to the PBX, and the OIT equipment and maintenance database, covering all items for which OIT has maintenance responsibilities. The PBX data are believed to be current and accurate (for equipment either currently in, or scheduled to be in, the Headquarters complex). Your staffs need only generally review this PBX survey equipment. Outbuilding listings, derived from the equipment database, however, require a more thorough review. The constant unreported movement of this equipment has caused inaccuracies in the database. In addition, there is a significant amount of component equipment not in the maintenance database due to the fact that OIT support was never requested.

4. Detailed census packages will be forwarded to your component (office) Automated Data Processing Control Officers (ADPCOs). Agency ADPCOs were briefed on the purpose, scope, methodology, and schedule of the census on 15 March at an Agency ADPCO meeting. Component ADPCOs have been requested to complete the census by providing current data in either an on-line or hardcopy format. In either case, we request that the data be forwarded through the Directorate ADPCOs and/or Management Staffs to my Management Services Division OIT, [redacted] by 10 June. Questions regarding the census may be directed to [redacted] of MSD/OIT.

5. I recognize that this census represents additional work for your staff. I apologize for adding to their burden but I believe establishing an accurate inventory justifies the increased workload. I expect that periodic updates to the inventory will go more smoothly once an accurate baseline is established. My staff has made a major effort to mitigate the Agency-wide impact and will provide your components with additional assistance should it be required. Please do not hesitate to contact me on secure [redacted] should you have further questions or concerns.

6. Thank you for your help in this matter.

[redacted]  
Edward J. Maloney

~~ADMINISTRATIVE - INTERNAL USE ONLY~~